

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

1073 Wheelers Church Road, Hurdle Mills, North Carolina
27541

Case No.

1:17MJ320-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The premises located at 1073 Wheelers Church Road, Hurdle Mills, North Carolina 27541, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)(A)	Distribution/Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit which is attached hereto and incorporated herein by reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

On this day,
 appeared before me via reliable electronic means, was
 placed under oath, and attested to the contents of this
 Application for a Search Warrant.

Sworn to before me and signed in my presence.

Date:

9/19/17 8:45 AM

City and state: Durham, North Carolina

TFO Thomas J. Ouellette

Applicant's signature

TFO Thomas Ouellette, F.B.I.

Printed name and title



Judge's signature

Joe L. Webster, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT APPLICATIONS

I, Task Force Officer (TFO) Thomas Ouellette of the Federal Bureau of Investigation (FBI), assigned to the Raleigh Residential Agency, being duly sworn, depose and state as follows:

INTRODUCTION

1. I graduated from SUNY Plattsburgh with a Bachelor of Arts in Criminal Justice in 1995. I have been a sworn law enforcement officer with the Raleigh Police Department since October of 1997 and have been assigned to the Investigations Division since April of 2004. During my career as a Detective, I have been assigned to numerous units, including the Juvenile Unit and the Special Victims Unit. In June 2014, I was sworn in as a Special Deputy U.S. Marshal assigned to the FBI. I am currently assigned to the FBI Child Exploitation Task Force and I am member of the North Carolina Internet Crimes Against Children (NCICAC) Task Force. As a member of these task forces, I investigate crimes involving child exploitation including the production and transportation of child pornography. I have received training in the investigation of sex crimes and computer related offenses through regular in-service training and outside training seminars. I have also received training through NCICAC in undercover communications with

adult offenders seeking sexual contact with juveniles and perpetrators seeking to trade and distribute images of child pornography. I have investigated numerous violations through the course of my duties as a Raleigh Detective and I have seized evidence and arrested persons for violations of state and federal laws. In my capacity as a Federal Task Force Officer, I am authorized to investigate violations of Federal laws and to apply for and execute Federal warrants.

2. This affidavit is submitted in support of applications for search warrants for the premises located at 1073 Wheelers Church Road, Hurdle Mills, North Carolina 27541 (the "SUBJECT PREMISES"), the person of KEVIN PATRICK FLAMEN, and a tan/beige 1999 Chrysler LHS sedan with North Carolina license plate PDW-2582 (the "SUBJECT VEHICLE") for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B of this affidavit.

3. The statements in this affidavit are based on information provided by Detectives with the Indianapolis Metropolitan Police Department, Google, state databases, internet service providers, and the Person County Sheriff's Office as well as my own investigation into this

matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES, in the SUBJECT VEHICLE, and on the person of KEVIN PATRICK FLAMEN.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to Attachment B and this Affidavit:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or

hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the

ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

j. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

k. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c)

masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

n. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

o. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a

user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

PROBABLE CAUSE

BACKGROUND

6. On June 25, 2017, Indianapolis Metropolitan Police Department (IMPD) Detective Sean McCurdy responded to a child abuse allegation and conducted an interview with an individual ("Witness-1"). Witness-1 informed Detective McCurdy that she received a message on Facebook Messenger informing her that her relative, John Paul Brashers, was abusing a young minor relative. Witness-1 said she asked for proof and then received multiple videos. The person sending the videos to Witness-1 said that Brashers loaded the videos on the internet and placed them in a chat room designed to show images of child pornography. Witness-1 opened up the videos and saw her minor relative ("Child Victim-1") and Brashers engaged in sexual sexually explicit conduct. Witness-1 reported that she could identify Brashers' voice in the videos and she saw his face in one of the videos.

7. Detective McCurdy reviewed the videos on Witness-1's phone. He saw that the videos showed a very young girl engaging in sexually explicit conduct with an adult male. Four of the videos showed Child Victim-1

performing oral sex on the adult male. The fifth video showed the adult male pushing/rubbing his penis against the vaginal and anus of Child Victim-1.

8. On June 26, 2017, Child Victim-1 was forensically interviewed. She stated that Brashers and another person have taken pictures of her naked. Child Victim-1 is now three years old.

9. With permission, IMPD Detective and FBI Task Force Officer Darin Odier reviewed Witness-1's Facebook messenger account to look at the material sent from the original reporting person. Detective Odier accessed the Facebook messenger account and observed that the original reporting person sent Witness-1 videos and screenshots from a Kik Messenger conversation involving the Kik user account "JP Brashers" Kik is a mobile chat application. The profile for the Kik account, "JP Brashers," included a picture of a male subject who Detective Odier recognized as Brashers.

10. Pursuant to a state search warrant, law enforcement recovered a black ZTE cellphone from Brashers' residence. Examination of the phone revealed a large amount of attribution evidence indicating that Brashers was the user of the device, including the presence of the Kik Messenger application utilizing the user name "JP Brashers". Further, law enforcement

recovered from the phone an additional video depicting Brashers and Child Victim-1 engaged in sexually explicit activity.

DISTRIBUTION OF CHILD PORNOGRAPHY TO THE USER OF
YELLOWIRON7399@GMAIL.COM

11. During the forensic examination of Brashers' phone, law enforcement observed an email thread beginning on May 9, 2017, sent through the Craigslist anonymous communication service. The communication was between user "John Paul Brashers," utilizing the email address "jpb131314@gmail.com" and another person. The conversation involved discussion of child exploitation. The other person asked Brashers "What get you off" and Brashers replied, "Taboo Incest/Daddy/daughter." The other person then asked Brashers to send him a video to the email address "yellowiron7399@gmail.com". Based on the context of the conversation, Detective Odier believed that Brashers sent a video of himself engaging in sexually explicit conduct to "yellowiron7399@gmail.com".

12. A federal search warrant was executed on Bashers' email account, "jpb131314@gmail.com". The "jpb131314@gmail.com" search warrant return from Google revealed that Brashers was distributing images and videos of Child Victim-1 engaged in sexually explicit conduct to multiple unknown people, including "yellowiron7399@gmail.com".

13. While reviewing the “jpb131314@gmail.com” search warrant return, Detective Odier observed the following:

a. On May 9, 2017, Brashers sent a video of himself engaging in sexually explicit conduct with Child Victim-1 (file name ending in 2379) to “yellowiron7399@gmail.com” via Craigslist’s communication service.

b. On May 16, 2017, Brashers sent a screenshot of a video of himself engaging in sexually explicit conduct with Child Victim-1 to “yellowiron7399@gmail.com”.

c. On May 18, 2017, Brashers sent a video of himself engaging in sexually explicit conduct with Child Victim-1 to “yellowiron7399@gmail.com”.

14. A federal search warrant was executed on the email account “yellowiron7399@gmail.com”. Upon review of the “yellowiron7399@gmail.com” search warrant return, Detective Odier located a May 9, 2017 email sent through Craigslist’s communications service by Brashers to “yellowiron7399@gmail.com”. Attached was a video depicting Brashers engaged in sexually explicit conduct with Child Victim-1.

15. Detective Odier also observed that the user of “yellowiron7399@gmail.com” was actively trading images of child pornography with other individuals including but not limited to:

a. On April 13, 2017, the user of an email address (“User-1”) sent the user of “yellowiron7399@gmail.com” multiple images of child pornography, including a file named “01ad494d-4ecb-4c76-a272-3fa652a3e394.jpg” depicting a naked adult male laying on a bed with a nude female child laying on top of the male. The male’s penis is against the exposed vaginal area of the child. Detective Odier observed at least twenty emails between User-1 and the user of “yellowiron7399@gmail.com” in which images of child pornography were exchanged.

b. On March 31, 2017, “yellowiron7399@gmail.com” sent the user of an email address (“User-2”) a file named “008dasdw.jpg” depicting a toddler female holding a male penis in her hand. A male hand is on the child’s head, her eyes are closed and she has what appears to be male ejaculate on her face. The user of “yellowiron7399@gmail.com” sent User-2 multiple emails with multiple

images of child pornography. User-2 thanked the user of “yellowiron7399@gmail.com” for the emails.

c. On March 30, 2017, “yellowiron7399@gmail.com” sent the user of an email address (User-3) a file named “002-82 (2).jpg” depicting a naked prepubescent female lying on her back with her legs spread apart as to expose her vaginal area.

d. On March 30, 2017, the user of an email address (User-4) sent “yellowiron7399@gmail.com” a file named “270x330_f5f205e7c8e5da752e60.jpg” depicting a prepubescent female standing in front of an adult male’s penis. The child is holding up her skirt exposing her vaginal area.

IDENTIFICATION OF FLAMEN AS THE USER OF
YELLOWIRON7399@GMAIL.COM:

16. While reviewing the results of the “yellowiron7399@gmail.com” search warrant return, Detective Odier observed several images of an adult male with a beard sent from “yellowiron7399@gmail.com” to other email accounts during the course of conversations. The images appear to be self-produced images commonly referred to as “selfies”. In email communications, the user of “yellowiron7399@gmail.com” referred to himself as “Kevin” and stated he works as an “auto tech”. Additional images within the

“yellowiron7399@gmail.com” return depict the same adult male wearing a commercial work shirt with the name “Kevin” clearly displayed on a patch attached to the shirt and a patch displaying the company name, “Mike’s Transmission Service”. During the investigation, it was discovered that some of the craigslist postings associated with “yellowiron7399@gmail.com,” were made from IP addresses geo-locating to the Raleigh, North Carolina area. An open source search showed “Mike’s Transmission Service” having shop locations in both Raleigh and Durham, North Carolina.

17. A further review of the “yellowiron7399@gmail.com” warrant return revealed that on multiple occasions the user of “yellowiron7399@gmail.com” provided the contact phone number (984) 234-9705 as a way for others to contact him. Using an open source search technique, law enforcement discovered that this phone number is associated with the Facebook account for “Kevin Flamen” (facebook.com/kevin.flamen). Examination of the publicly accessible Facebook page in question revealed images depicting what appears to be the same male subject depicted in the selfies described immediately above.

18. A name search of the North Carolina Division of Motor Vehicles (DMV) database yielded a match for the subject, Kevin Patrick FLAMEN

(DOB 12/13/1975) of 1073 Wheelers Church Road, Hurdle Mills, North Carolina 27541 (the SUBJECT PREMISES). The driver's license photo of FLAMEN on file with the DMV appears to depict the same person as the above-described selfies and "Kevin Flamen" Facebook images.

19. An employment history check for FLAMEN revealed that he is employed at "Mike's Transmission Service" located at 836 N. Mangum Street, Durham, North Carolina 27701. This is consistent with the work shirt patch observed in one of the aforementioned selfie images.

20. IP connectivity logs provided by Google for "yellowiron7399@gmail.com" reveal at what time and from what IP address the user of "yellowiron7399@gmail.com" accessed the email account. My review of these logs reveals that the user logged into the email account on multiple dates and times from different IP addresses. Based on my experience investigating internet crimes, it is typical to observe multiple logins to social media applications and/or email accounts on multiple dates and times from different IP addresses due to the portability of mobile devices (e.g. smartphones, laptops, tablets, and other mobile devices).

21. Google provided IP connectivity logs for "yellowiron7399@gmail.com" from March 8, 2017 through June 28, 2017. The

majority of the login IP addresses for “yellowiron7399@gmail.com” during this time are 174.109.104.18, assigned to Charter Communications, and other IP address assigned to AT&T Mobility, a mobile device internet provider.

22. A subpoena issued by the Marion County Prosecutors Office in Indiana was served on Charter Communications for the account subscriber information for IP address 174.109.104.18 on relevant dates. On August 22, 2017, Charter Communications, Inc. responded to the administrative subpoena and identified the internet account as belonging to “ANY HOLMES OIL COMP” at 2716 Guess Road, Durham, North Carolina 27705. I identified this address as a Cruizers Convenience Marketplace located only a few blocks from Mike’s Transmission Service.

23. During my review of the IP connectivity Logs, I observed that, on June 13, 2017, the user of “yellowiron7399@gmail.com” logged in from IP address 50.111.24.191. This IP address was issued to Frontier Communications. On September 1, 2017, I issued an administrative subpoena to Frontier Communications requesting the subscriber information associated with IP address 50.111.24.191 on June 13, 2017.

24. On September 1, 2017, Frontier Communications responded to the administrative subpoena and identified the internet account as belonging

to "Mike's Transmission Service" located at 836 N. Mangum Street, Durham, North Carolina 27701.

25. Based on the above information, I believe that Kevin Patrick FLAMEN (DOB 12/13/1975) of 1073 Wheelers Church Rd, Hurdle Mills, North Carolina 27541, is the user of "yellowiron7399@gmail.com".

26. North Carolina DMV records reveal that FLAMEN owns a tan/beige 1999 Chrysler LHS sedan with North Carolina license plate PDW-2582 (the "SUBJECT VEHICLE").

27. Based on the investigation, on August 29, 2017, Detective Darin Odier presented a criminal complaint to Magistrate Judge Mark J. Dinsmore in the Southern District of Indiana charging FLAMEN with knowingly receiving depictions of a minor child engaged in sexually explicit conduct in violation of 18 U.S.C § 2252(a)(2). After reviewing the probable cause stated in the criminal complaint, Magistrate Judge Dinsmore issued an arrest warrant for FLAMEN charging him with a violation of 18 U.S.C § 2252(a)(2). The complaint and arrest warrant are currently under seal.

28. On August 31, 2017, I conducted surveillance on the SUBJECT PREMISES. The SUBJECT PREMISES is situated in Person County within the Middle District of the State of North Carolina. The residence is a one

story wooden structure, single family home, with gray/blue colored siding with white colored trim, and a front porch. The numbers "1073" are posted on the mailbox situated at the end of the driveway associated with the residence. The main entrance appears to be the door situated on the front of the house facing Wheelers Church Road accessible via the front porch.

29. On or around September 2, 2017, law enforcement officers from the Person County Sheriff's Office in North Carolina observed a tan colored Chrysler sedan at the SUBJECT PREMISES. On September 12, 2017 at approximately 11:00 PM, additional surveillance revealed that the SUBJECT VEHICLE was parked in the driveway of the SUBJECT PREMISES.

30. Brashers gave law enforcement permission to access and take control of his online accounts. This included the email address, jpb131314@gmail.com. On September 11, 2017, Brashers email account, "jbp131314@gmail," received an email from "Yellowiron7399@gmail.com," that read, "Hey". On September 12, 2017, operating in an undercover capacity, Detective Odier responded "Hey". The user of the email, "Yellowiron7399@gmail.com" replied, "What's up man hit me with something good." Det. Odier replied, "Shes with her mom till next weekend. Got something for me?" On September 13, 2017, at 12:38 PM, the email,

“jpb131314@gmail.com,” received an email from “Yellowiron7399@gmail.com” which contained an attachment titled, “IMG_1023.png.” The image depicts an infant or toddler aged female lying on a bed with her legs in the air. An adult hand is seen spreading the child’s exposed vaginal area.

31. On September 13, 2017, around 2:20 PM, surveillance was conducted on Mike’s Transmission Service, located at 1031 Corporation Pkwy, Raleigh, NC 27610, and the SUBJECT VEHICLE was observed parked in the parking lot.

32. On September 14, 2017, around 5:10 AM, surveillance was conducted on the SUBJECT PREMISES and it was discovered that the subject vehicle was not present at the time.

33. On September 14, 2017, around 7:15 AM, additional surveillance was conducted on Mike’s Transmission Service 1031 Corporation Pkwy, Raleigh NC, and the SUBJECT VEHICLE was observed parked in the parking lot, but in a different parking spot than on September 13, 2017.

34. On September 14, 2017, around 11:00 PM, law enforcement officers from the Person County Sheriff’s Department conducted surveillance on the SUBJECT PREMISES and observed the SUBJECT VEHICLE was parked in the driveway.

35. On September 15, 2017, law enforcement officers from the Person County Sheriff's Department conducted surveillance on the SUBJECT PREMISES and observed the SUBJECT VEHICLE leave the SUBJECT PREMISES around 4:50 AM.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO TRAFFIC IN
AND POSSESS CHILD PORNOGRAPHY**

36. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who traffic in and possess child pornography:

- a. Such individuals often receive sexual gratification from viewing child pornography.
- b. The majority of such individuals view child pornography on their computers or mobile devices via the internet.
- c. Such individuals almost always hide their viewing and storage of child pornography from their loved ones and other household members.

d. Such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as on a computer, thumb drives, external hard drives, and mobile devices. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. In many instances these types of files have been found stored for years and transferred between electronic devices.

e. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

37. I believe that the user of “yellowiron7399@gmail.com”, Kevin Patrick FLAMIN displays characteristics common to individuals who traffic in and possess child pornography. I believe this because a review of his email account reveals that FLAMIN exchanged multiple child pornography files with numerous other individuals.

**BACKGROUND ON COMPUTERS, CHILD PORNOGRAPHY,
THE INTERNET, AND EMAIL**

38. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally

millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are

very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online

storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. With the advent of mobile devices (*i.e.* "smart" cell phones, tablets, PDAs ...) which can access the internet through a multitude of different applications, individuals engaged in the viewing, storing, and trading of child pornography have been able to access, store, and trade

these images using their cell phones. Mobile devices are essentially mini-handheld computers with most of (or all of) the functionality of a traditional computer including email. Mobile devices can utilize applications for remote storage services (like Dropbox, MediaFire, and OneDrive accounts) to access, view, store, and share digital files with others, including images of child pornography. Mobile devices can also be used to communicate with others through various chat applications such as Kik.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. As described in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in the SUBJECT VEHICLE, and on the person of the SUBJECT INDIVIDUAL in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on the person of the

SUBJECT INDIVIDUAL there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

41. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks,

magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to cloud-based storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly

vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography

a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

42. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence

listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

FINGERPRINT UNLOCK AUTHORIZATION

43. As described above, a significant number of the IP addresses associated with “yellowiron7399@gmail.com” resolve to AT&T Mobility and thus a mobile device. I know from my training and experience, as well as from information found in publicly available materials that some mobile devices offer their users the ability to unlock the device via the use of a

fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. In the case of Apple products, this feature is called Touch ID.

44. The passcode or password that would unlock the mobile device(s) possessed by FLAMEN are not known to law enforcement. Thus, it may be necessary to press the finger(s) of the user(s) of the mobile devices seized pursuant to this search warrant to the device’s fingerprint sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. This is necessary because the government may not otherwise be able to access the data contained on the mobile device(s) for the purpose of executing the search authorized by this warrant.

45. Consequently, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Kevin Patrick FLAMEN (DOB 12/13/1975) to the fingerprint sensor of any mobile device recovered pursuant to this search warrant for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

SEARCH EXECUTION PRIOR TO 6:00 AM

46. I, with other law enforcement officers, plan to serve a warrant for FLAMEN'S arrest upon him soon after he leaves his home for work in the morning. Based on surveillance and the location of his residence and employer, I believe that FLAMEN regularly departs his home for work at approximately 5:00 AM. Therefore, I expect FLAMEN to be taken into custody between 5:00 and 6:00 AM the day the requested search warrants will be executed. Consequently, good cause having been shown, I request authority to execute the search warrants on FLAMEN and the SUBJECT VEHICLE between 5:00 AM and 10:00 PM.


CONCLUSION

47. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT PREMISES described in Attachment A, in the SUBJECT VEHICLE, and on the SUBJECT PERSON. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, SUBJECT VEHICLE, and SUBJECT

PERSON authorizing the seizure and search of the items described in Attachment B.

TFD Thomas J. Ouellette
Detective T.J. Ouellette
Task Force Officer
Federal Bureau of Investigation

Sworn and subscribed before me this 19th day of September, 2017. 8:45AM.



Joe L. Webster
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

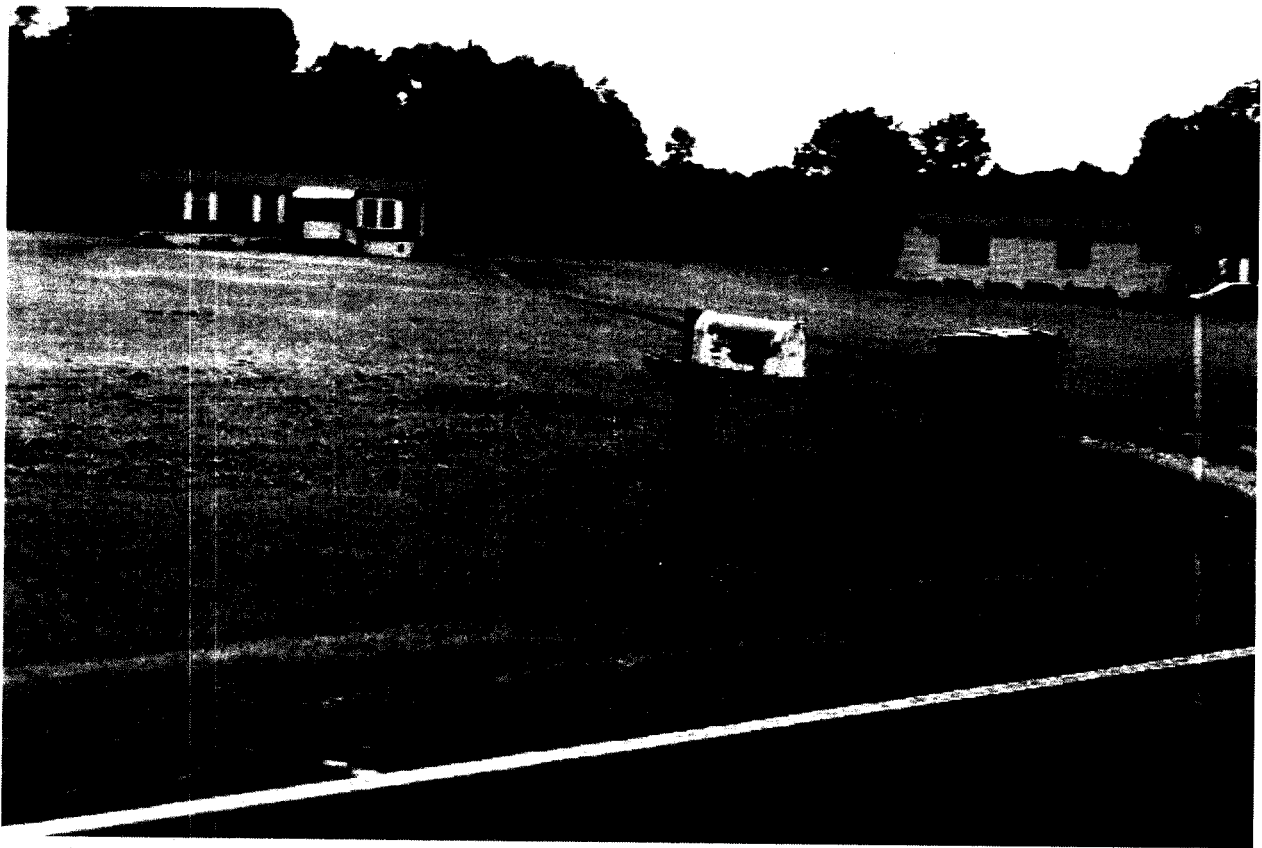
1073 WHEELERS CHURCH RD, HURDLE MILLS, NC 27541

Premises to Be Searched

The premises located at **1073 WHEELERS CHURCH RD, HURDLE MILLS, NC 27541**, is situated in Person County within the Middle District of the State of North Carolina. The residence is a one story wooden structure, single family home, with gray/blue colored siding with white colored trim, and a front porch. The numbers "1073" are posted on the mailbox situated at the end of the driveway associated with the residence. The main entrance appears to be the door situated on the front of the house facing Wheelers Church Rd accessible via the front porch. An area map and photographs of the premises are incorporated herein.

ATTACHMENT A

1073 WHEELERS CHURCH RD, HURDLE MILLS, NC 27541
SUBJECT PREMISES:



ATTACHMENT A

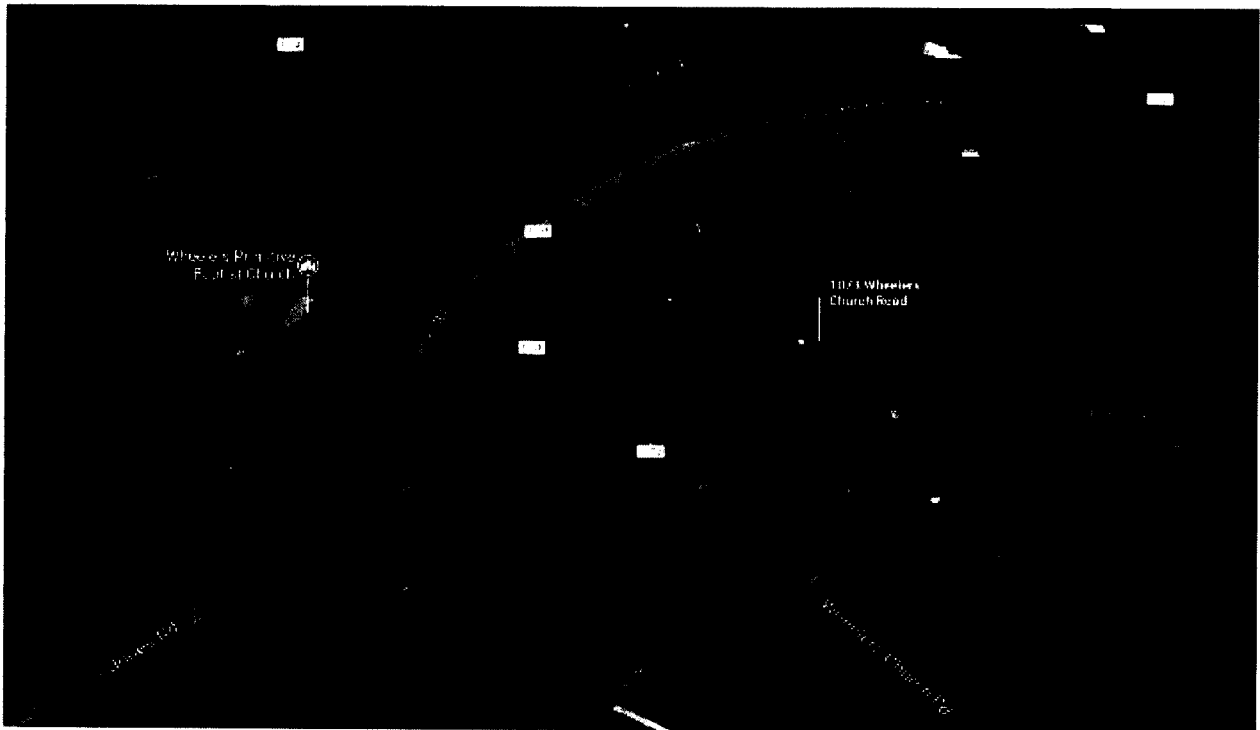
1073 WHEELERS CHURCH RD, HURDLE MILLS, NC 27541



ATTACHMENT A

1073 WHEELERS CHURCH RD, HURDLE MILLS, NC 27541

Satellite map of area:



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251(a) and 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of

malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
- e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- f. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- g. evidence of the times the COMPUTER was used;
- h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- j. records of or information about Internet Protocol addresses used by the COMPUTER;
- k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

- cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content and/or the identity of the computer user; and
3. Routers, modems, and network equipment used to connect computers to the Internet.
 4. Child pornography and child erotica.
 5. A commercial work shirt with the name “Kevin” displayed on a patch attached to the shirt and a patch displaying the company name, “Mike’s Transmission Service.
 6. Records, information, and items relating to violations of the statutes described above in the form of:
 - a. Records, information, and items referencing or revealing the ownership or use of computer equipment found at 1073 Wheelers Church Road, Hurdle Mills, North Carolina 27541, in a 1999 Chrysler LHS Sedan NC License Plate: PDW-2582, and on the person of Kevin Patrick Flamen;
 - b. Records and information referencing or revealing the identity of the user of “yellowiron7399@gmail.com.”
 - c. Records and information referencing or revealing the sexual exploitation of children, including communication between

individuals engaged in the advertisement, receipt, distribution and production of child pornography;

- d. Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography;
 - e. Records and information revealing sexual activity with or sexual interest in minors;
 - f. Correspondence and communications of an illicit sexual nature with minors; and
 - g. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage.
7. During the course of the search, photographs of the residence may be taken to record the condition thereof and/or the location of items therein.
8. During the course of the search warrant, law enforcement officers may press the fingers (including thumbs) of Kevin Patrick FLAMEN (DOB 12/13/1975) to the fingerprint sensor of any mobile device recovered pursuant to this search warrant for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.